

REMARKS

Reconsideration of the holdings in the Office Action mailed from the PTO on May 7, 2004 is respectfully submitted.

Claim Rejections - 35 USC § 112

"Claims 7-10 are rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 7 and 8 recites the word "them". There s a lack of clarification as to what "them" refers to in the claim. Appropriate correction is required. Claims 9-10 are dependents of claim 7 and inherit the same reasons of rejection."

Applicant's Response

Claims 7 and 8 have been amended to correct for the stated lack of clarity. Therefore, claims 7-10 should be allowed.

Priority

The specification is amended to show relation to priority application.

Drawings

The drawings are objected to because they include a reference sign not mentioned in the description: 18 of figure 1.

Applicant's Response

The reference number 18 is given on page 5, line 35 of the specification, and shown in Figure 1 with a line leading to box CRC, written in box 7.

Claim Rejections - 35 USC § 103

"Claims 1, 5-8 and 11 are rejected under 35 USC 103(a) as being unpatentable over Geroniomi et al (hereinafter Geroniomi), US Patent 5,629,513, in view of Yu et al (hereinafter Yu), US Patent 6,067,621."

Applicant's Response

The aim of the present invention is to provide a method for testing an integrated circuit which comprises confidential parts to be protected from an unauthorized person. The

Amendment A
ICB-0038

Page 8 of 14

confidential parts of said integrated circuit are for example algorithms, programs, test procedures stored in a memory ROM and/or RAM. For allowing access to confidential parts of the integrated circuit for a specific tester, a barrier of the integrated circuit has to be opened. For that, a first password is obtained in the integrated circuit on the base of a random number generated by a random number generator and a ciphering of this random number with a stored key by a ciphering algorithm, and a second password is obtained in the tester in parallel on the base of the random number provided by the integrated circuit and a ciphering of this random number with a same key by an identical ciphering algorithm. Finally, the first and second passwords are compared in a comparator of the integrated circuit in order to open the barrier in case of match of said two passwords to allow access to confidential parts to be tested. It is to be noted that each processed password is different subsequent to each connection of the tester to the integrated circuit, and if the two passwords are different after the comparison, the barrier is not closed.

The patent US 5,629,513 of Geroniomi describes a method for the functioning of a chip card in different steps of manufacturing and customizing of the chip as well as its use, however, it does not describe a method for testing an integrated circuit as claimed in the present invention. The manufacturer has to have access to all the non-volatile memory zones of the chip, which is different from the final chip card user. For that, there is a barrier in the chip to protect confidential parts. In case of malfunctioning of the chip, in particular in the confidential parts, it is necessary to allow repairing these zones of the chip by opening the barrier.

The chip card further comprises a first state indicator for the life cycle in which the chip card is located, and a second state indicator for defining the right to return to a previous step. The first indicator is changed from a first value to a second value during the passage of the card from a first state to a second state in order to prohibit reading certain confidential parts of the chip card. This first indicator can be reset at its first state under control of the second indicator. So the second indicator can be set at the first value for the return of the first indicator to its first value under control of a return instruction applied to the card. However if the second indicator is placed at its second value, this prohibits the return of the first indicator at its first value, which is different from the present invention.

By setting the second indicator in its first value, the card reader has to calculate parameters with an enciphering algorithm and a key. A command with these parameters is sent to the chip card and checked in the chip card by an operating system (col. 4, l. 35-40) to return to a previous step if the parameters are correct, i.e. correspond to those that are expected (col. 4, l. 44-49). These parameters, sent by the reader, can be calculated on the base of the number of the card. The operating system of the card verifies the parameters with the same computation as the reader.

In contrast to the present invention, the Geroniomi's patent is not intended to execute a test of the integrated circuit. Furthermore, the use of a random number, which change at each connection of the tester to the integrated circuit, for calculating the passwords allows a great security of the integrated circuit, which is different from the method of Geroniomi's patent in which the opening of the barrier can be done only if the parameters of the reader are correct, otherwise the confidential parts are definitively closed. The computation is effected with a number of the card and not with a random number supplied once the tester is connected to the integrated circuit as the presently claimed invention. Even if a computation in the operating system is equivalent to a computation in the card reader, it is not mentioned in the Geroniomi's patent if the computation is effected in parallel of the computation in the card reader as specified in claim 1 of the present invention. Furthermore, it is not indicated how the comparison is executed in the chip card, whereas the integrated circuit of the present invention indicates that the first password is placed in a password register, and a comparison by comparing means between the two passwords controls the opening or closing of the barrier.

As with the use of the random number generator for providing a random number when the tester is connected to the integrated circuit, this is required to execute the computation in parallel, which assures a great security to allow only the use of a specific tester to open the barrier of access to confidential parts, which is contrary of Geroniomi's patent. Thus, amended claims 1, 7 and 11 are novel.

The patent US 6,067,621 (Yu et al), published after the priority date of the above-mentioned patent application, describes a user authentication system for authenticating an

authorized user of a chip card. An integrated circuit card with a portable terminal are used in combination for conducting financial transactions in connection to a server. For a greater security, a one-time password can be used in order to be changed each time the user wishes to be authenticated. The integrated circuit card comprises in particular a stored secret key for generating a one-time password in the terminal, and predetermined random numbers. The terminal, in which the IC card is inserted, comprises in particular a first changer of random numbers, and a first password generator to generate a one-time password using the IC card as an input. The server connected to the terminal comprises a second random number changer and a second password generator in order to generate a same one-time password for the authentication of the user of the card.

In contrast to the present invention, Yu's patent does not describe a method for testing an integrated circuit including confidential parts in particular after step of manufacturing of said integrated circuit. Furthermore, the random number generators are not used to open a barrier of the integrated circuit, which protects confidential parts of the integrated circuit, but only to change the password for greater security during financial transactions. So the integrated circuit card does not comprise a random number generator to produce a random number transmitted to a tester as in the presently claimed invention.

At the light of the teaching of Geroniomi's patent combined with Yu's patent, a man skilled in the art would show imagination, if he thought using a random number generator in the integrated circuit for producing a specific random number when the tester is connected to the integrated circuit in test mode, in order to compute a first password on the base of said random number in the integrated circuit and a second password on the base of said received random number in the tester with a same method. The two passwords are checked in the integrated circuit by comparing means to open the barrier if the comparison establishes a match between the two passwords, which is neither described nor suggested in the Geroniomi's patent, when combined with the Yu's patent. Furthermore, this barrier is not closed if the two compared passwords are not the same at the difference of the card of Geroniomi's patent. Accordingly, it is respectfully submitted that claims 1, 7 and 11 are novel and based on an inventive step. It is the same situation for claims 8 and 9, which are neither described nor suggested by the two cited references.

Amendment A
ICB-0038

Page 11 of 14

Claim Rejections - 35 USC § 103**Continued**

"Claims 2-3, 10 and 12-13 are rejected under 35 USC 103(a) as being unpatentable over Geroniomi et al (hereinafter Geroniomi), US Patent 5,629,513, in view of Yu et al (hereinafter Yu), US Patent 6,067,621, as applied to claim 1 above, and further in view of Lewis, US Patent 5,875,248."

Applicant's Response

The patent US 5,875,248 (Lewis) describes a method of counterfeit detection of electronic data stored on a chip. A non-volatile memory is provided with a counterfeit detection mechanism by storing an encryption key protected in order to be not exported, and performing cryptographic operations on chip. The data processing system includes a processor card connected to several memory cards, which have each a stored key. However in the cited Lewis' patent, there is not mentioned a method for testing an integrated circuit and the use of third and fourth passwords calculated with a random number as set forth in claims 2, 3, 12 and 13 of this patent application.

Claim Rejections - 35 USC § 103**Continued**

"Claim 4 is rejected under 35 USC 103(a) as being unpatentable over Geroniomi et al (hereinafter Geroniomi), US Patent 5,629,513, in view of Yu et al (hereinafter Yu), US Patent 6,067,621, in view of Lewis, US Patent 5,875,248, and further in view of Fukawa, US Patent 6,112,187."

"Claim 9 is rejected under 35 USC 103(a) as being unpatentable over Geroniomi et al (hereinafter Geroniomi), US Patent 5,629,513, in view of Yu et al (hereinafter Yu), US Patent 6,067,621, and further in view of Bonneau et al. (hereinafter Bonneau), US Patent 6,577,229."

Applicant's Response

The patent US 6,112,187 (Fukawa), published after the priority date of this patent application, describes an encryption communication device able to improve the generation of a password without describing the features of claim 4 of the present invention. Finally, the patent US 6,577,229, granted after the filing date of this patent application, describes a

Amendment A
ICB-0038

Page 12 of 14

multiple protocol smart card communication device. This patent mentions an EEPROM memory, according to claim 9 of the present invention, but does not relate to a method for testing an integrated circuit, the integrated circuit and the tester for implementing the method of the present invention.

It is respectfully submitted that the combination of three or more documents submitted under 35 U.S.C. 103(a), suffers from a lack of proper motivation. In re Vaeck, 20 USPQ2d, 1438, 1442 (Fed. Cir. 1991), the federal circuit held that:

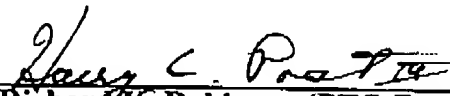
- The prior art must suggest to those skill in the art that they should make the claimed method or integrated circuit,
- The prior art must also reveal that in so making those skill would have a reasonable expectation of success, and
- Both the suggestion and the reasonable expectation of success must be founded in the prior art and not in applicant's disclosure.

Conclusion

For the foregoing reasons, it is respectfully submitted that Claims 1-15 are in condition for allowance, and such is respectfully requested.

Respectfully submitted,

Date: September 7, 2004


Richard K. Robinson (PTO Reg. No. 28,109)
Harry C. Post, III (PTO Reg. No. 26,019)
Attorneys for Applicant

Robinson & Post, L.L.P.
North Dallas Bank Tower, Suite 575
12900 Preston Road, LB-41
Dallas, Texas 75230
Tel: 972-866-7786
Fax: 972-866-7787